تكوين مصادقة المستخدم المستندة إلى RADIUS و TACACS

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

مصادقة المستخدم المستندة إلى RADIUS والتخويل ل vEdge ووحدات التحكم

مصادقة المستخدم والتفويض القائمين على TACACS ل vEdge ووحدات التحكم

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة المستخدم المستندة إلى TACACS و radius ل vEdge ووحدات التحكم باستخدام ISE.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

للأغراض الإيضاحية، يتم إستخدام الإصدار 2.6 من ISE. vEdge-cloud ووحدات التحكم التي تشغل الإصدار 19.2.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

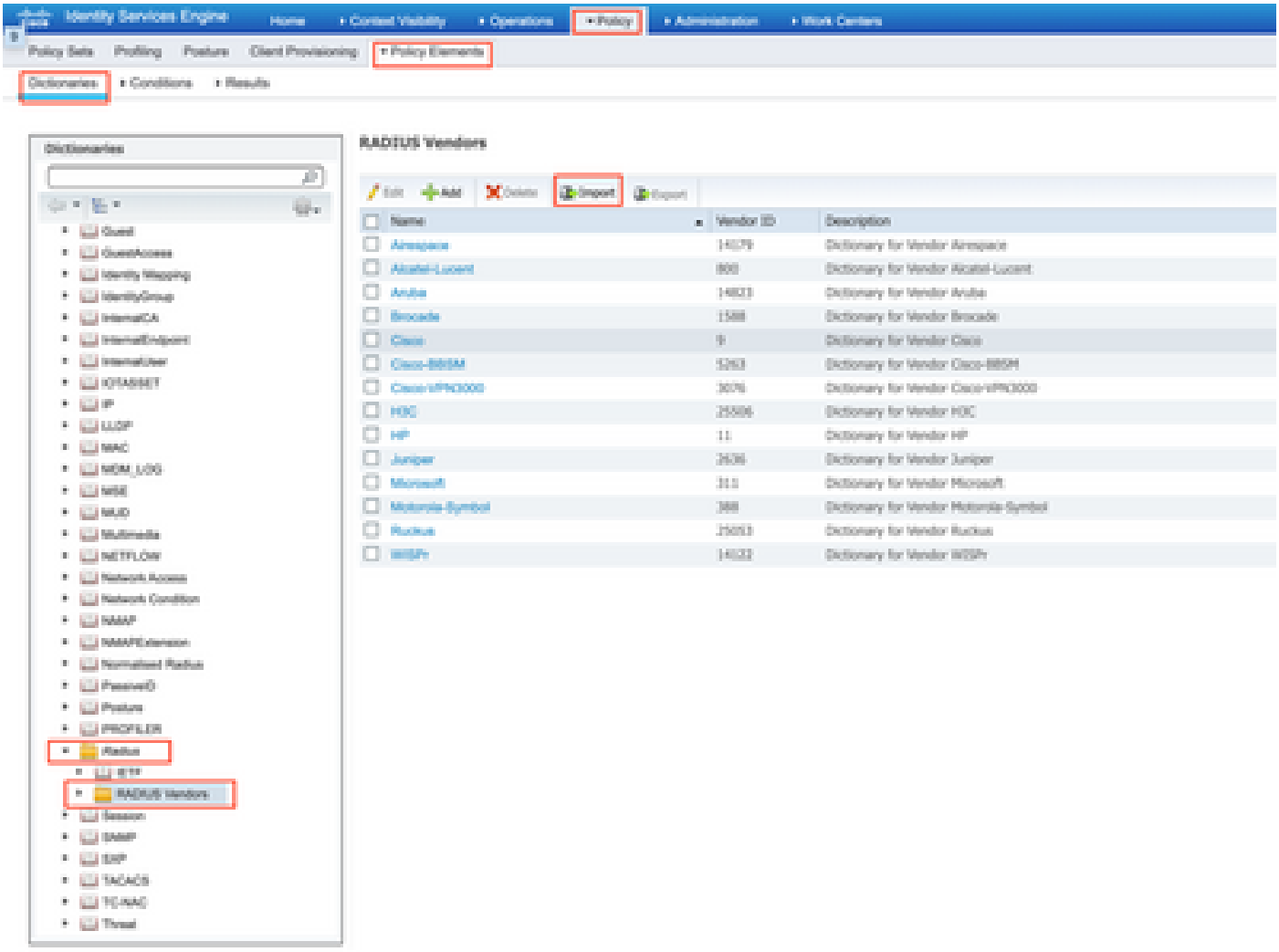
يوفر برنامج Viptela ثلاثة أسماء لمجموعات المستخدمين الثابتة: basic، netadmin، وoperator. يجب تعيين المستخدم لمجموعة واحدة على الأقل. يتم وضع مستخدم TACACS/RADIUS الافتراضي تلقائيا في المجموعة الأساسية.

مصادقة المستخدم المستندة إلى RADIUS والتخويل ل vEdge ووحدات التحكم

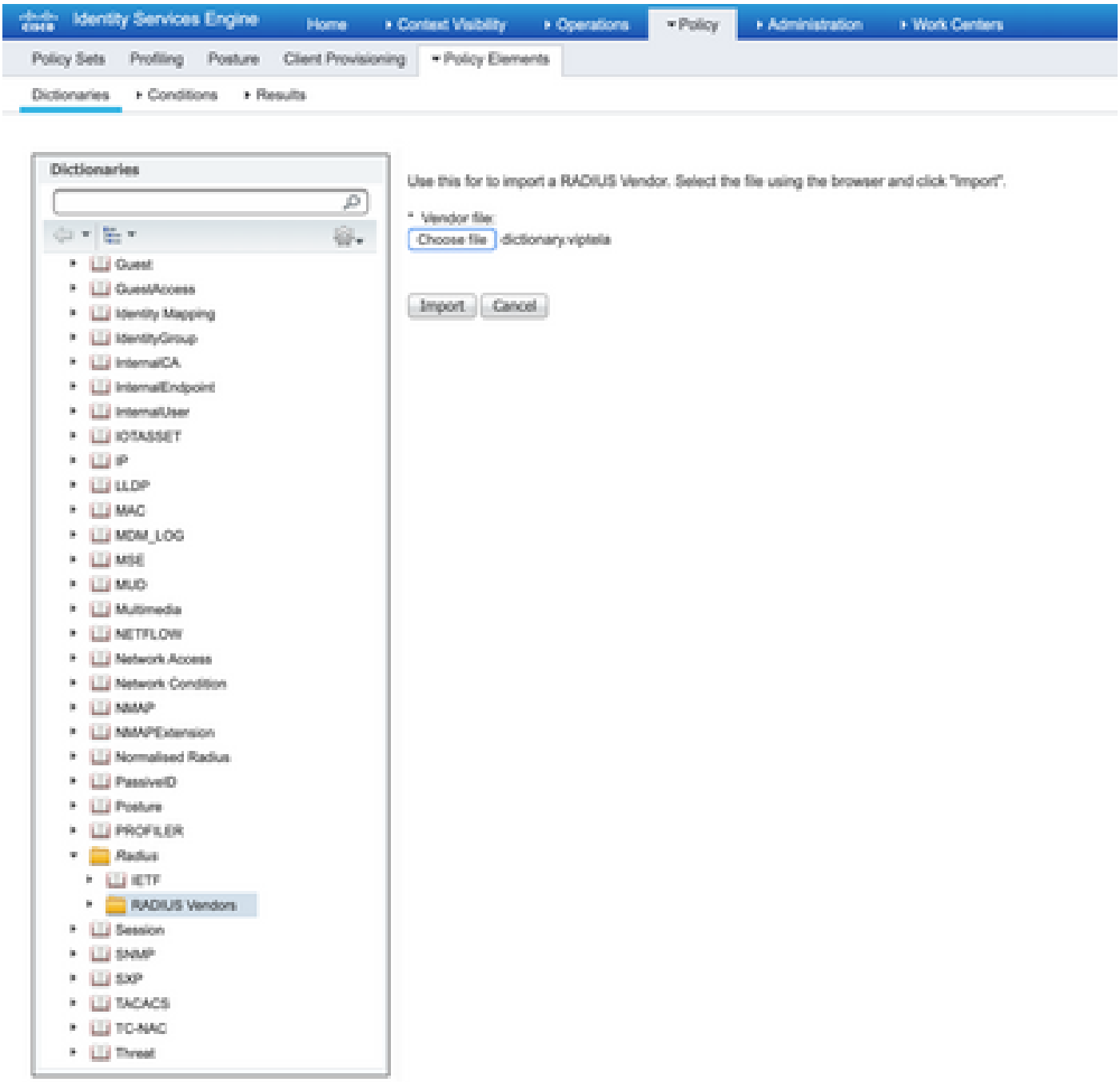
الخطوة 1. قم بإنشاء قاموس Viptela radius ل ISE. للقيام بذلك، قم بإنشاء ملف نصي بالمحتوى:

```
# -*- text -*-
#
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

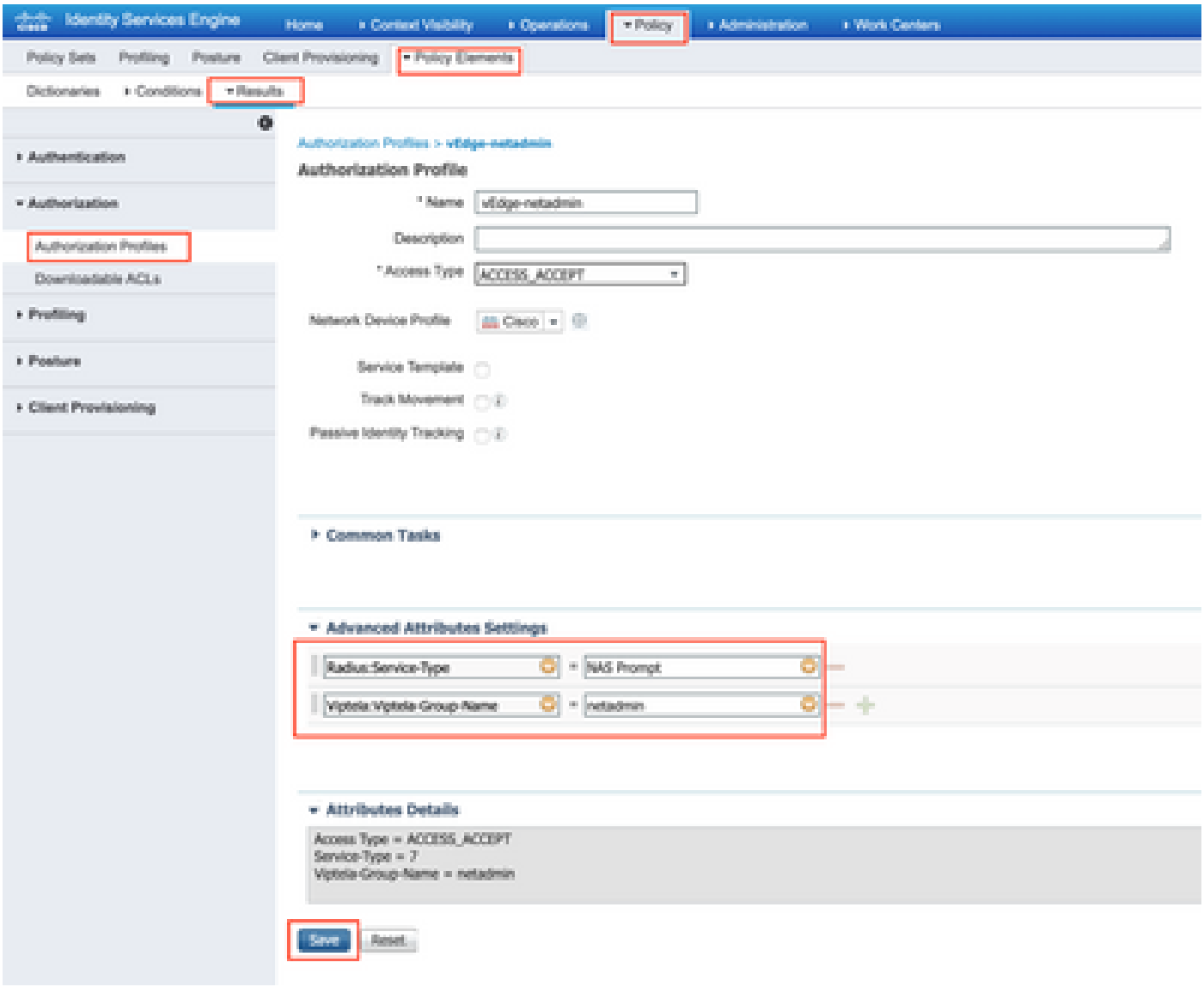
الخطوة 2. تحميل القاموس إلى ISE. لهذا الغرض، انتقل إلى السياسة > عناصر السياسة > القواميس. من قائمة القواميس، انتقل إلى Radius > موردي RADIUS ثم انقر إستيراد كما هو موضح.



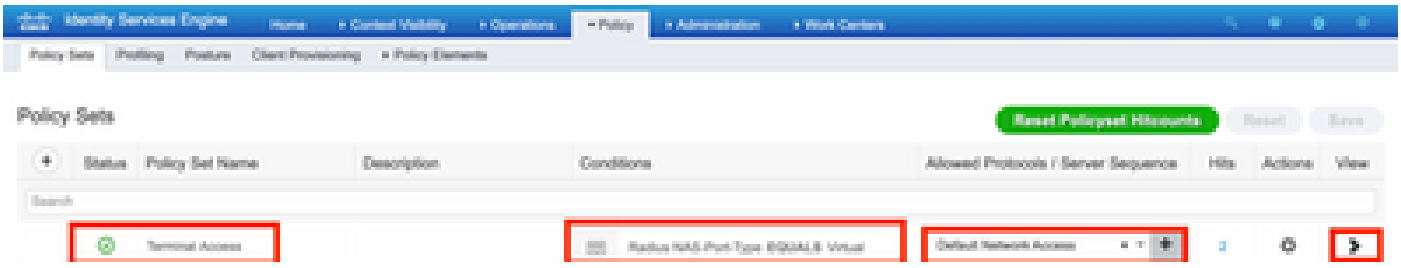
قم بتحميل الملف الذي أنشأته في الخطوة 1.



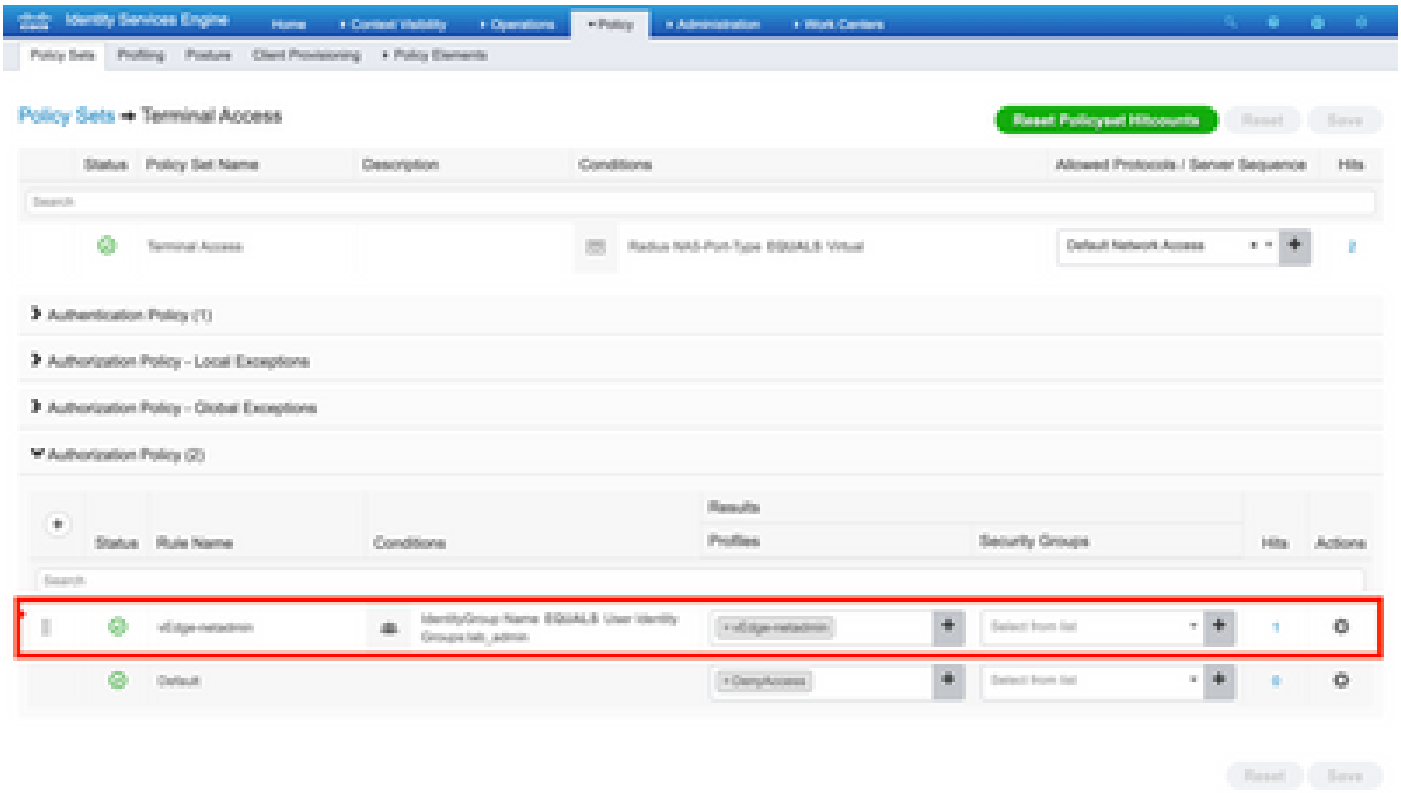
الخطوة 3. إنشاء ملف تعريف تخويل. في هذه الخطوة، يقوم ملف تعريف تخويل RADIUS، على سبيل المثال، بتعيين مستوى امتياز NetAdmin لمستخدم مصدق عليه. لهذا، انتقل إلى سياسة > عناصر السياسة > ملفات تخصيص التخويل وحدد خاصيتين متقدمتين كما هو موضح في الصورة.



الخطوة 4. قد تبدو مجموعة النهج بشكل مختلف وفقا للإعداد الفعلي الخاص بك. لأغراض العرض التوضيحي في هذه المقالة، يتم إنشاء إدخال السياسة الذي يسمى الوصول الطرفي كما هو موضح في الصورة.

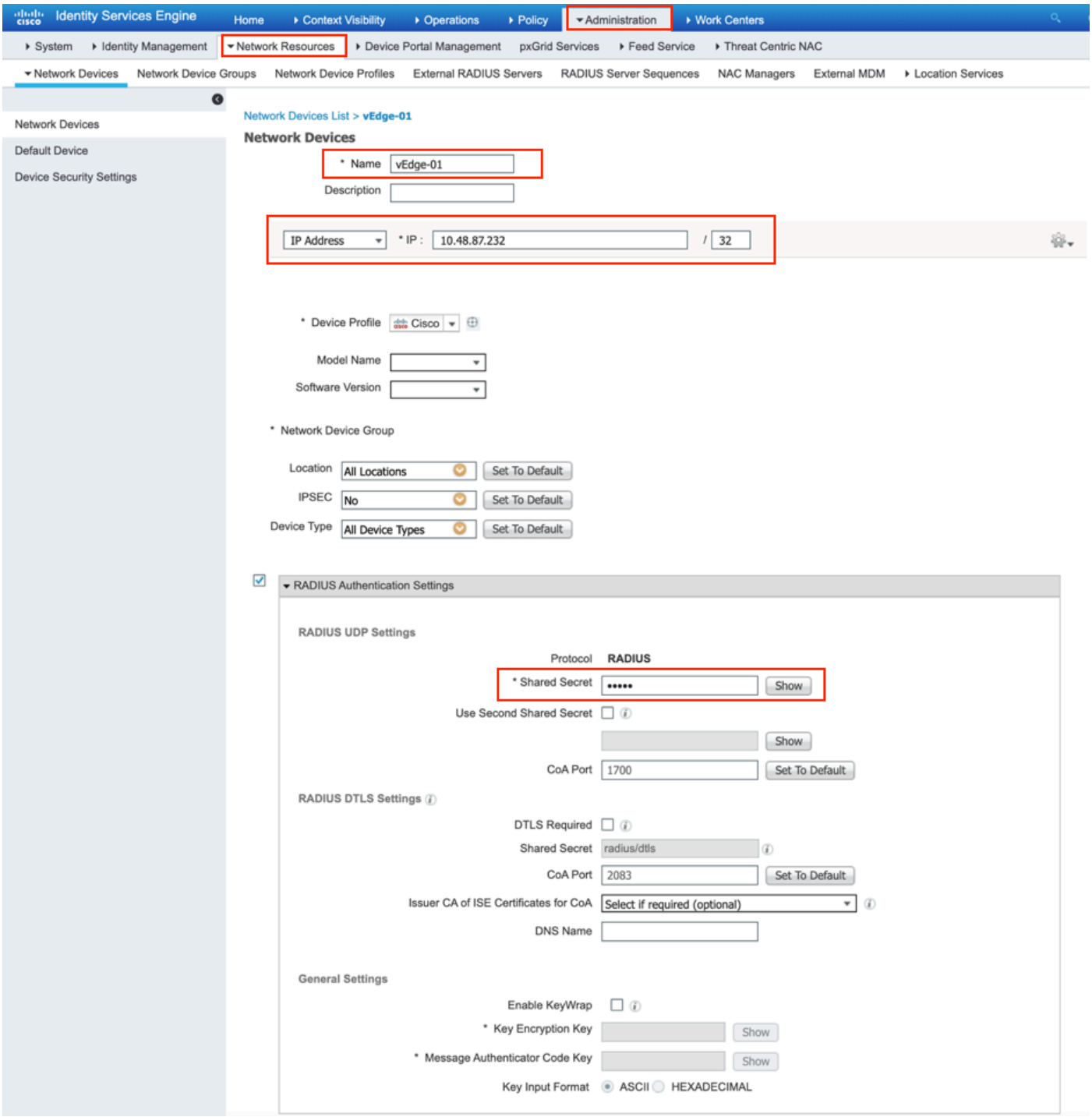


انقر > وتظهر الشاشة التالية كما هو موضح في الصورة.



يتطابق هذا النهج استنادا إلى ملف تعريف مجموعة المستخدمين lab_admin ويعين ملف تعريف تخويل تم إنشاؤه في الخطوة 3.

الخطوة 5. قم بتعريف NAS (موجه أو وحدة تحكم vEdge) كما هو موضح في الصورة.



الخطوة 6. تكوين vEdge/وحدة التحكم.

```
system
 aaa
  auth-order       radius local
  radius
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

الخطوة 7. التحقق. قم بتسجيل الدخول إلى vEdge وتأكد من تعيين مجموعة NetAdmin للمستخدم البعيد.

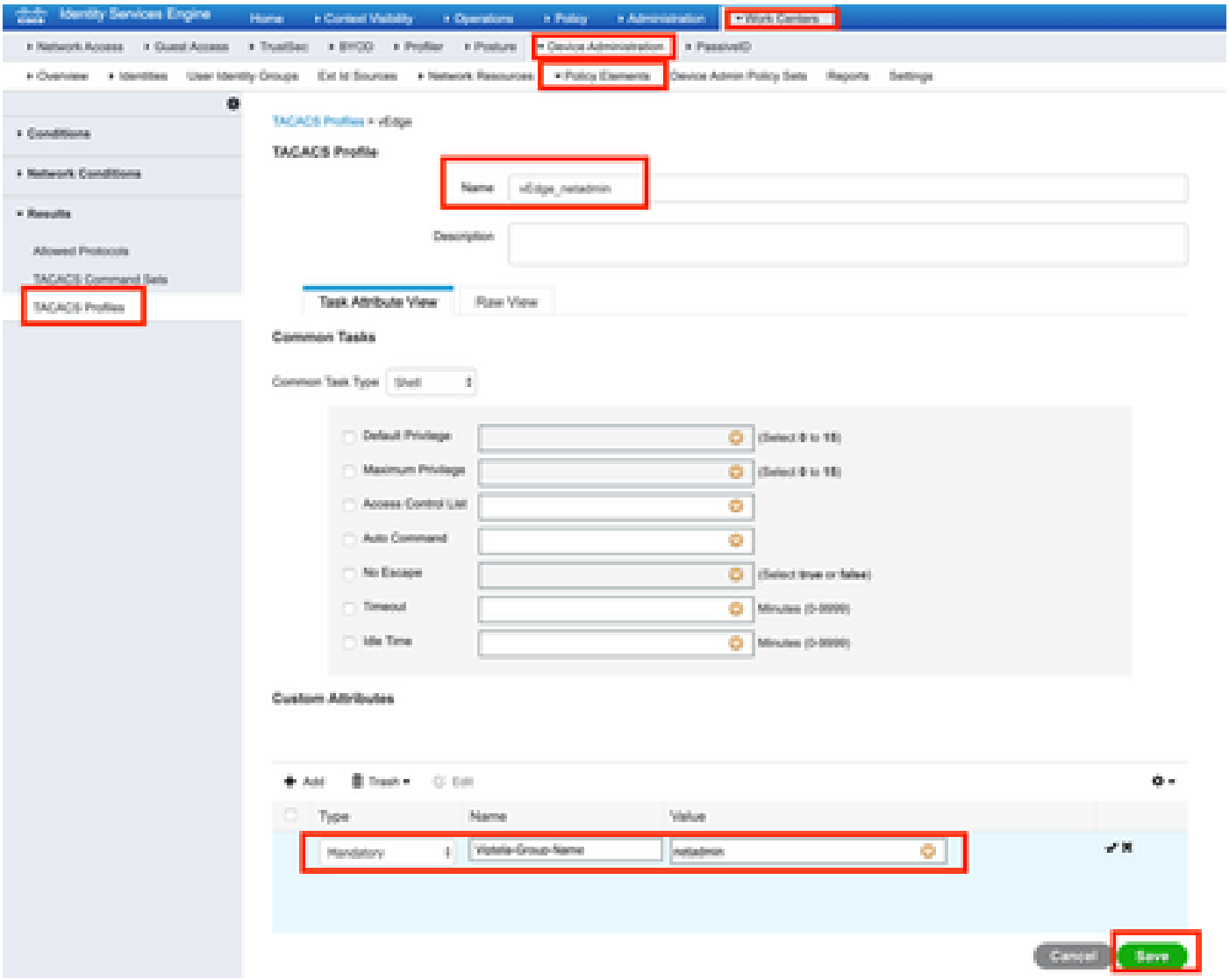
```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

مصادقة المستخدم والتفويض القائمين على TACACS لـ vEdge ووحدات التحكم

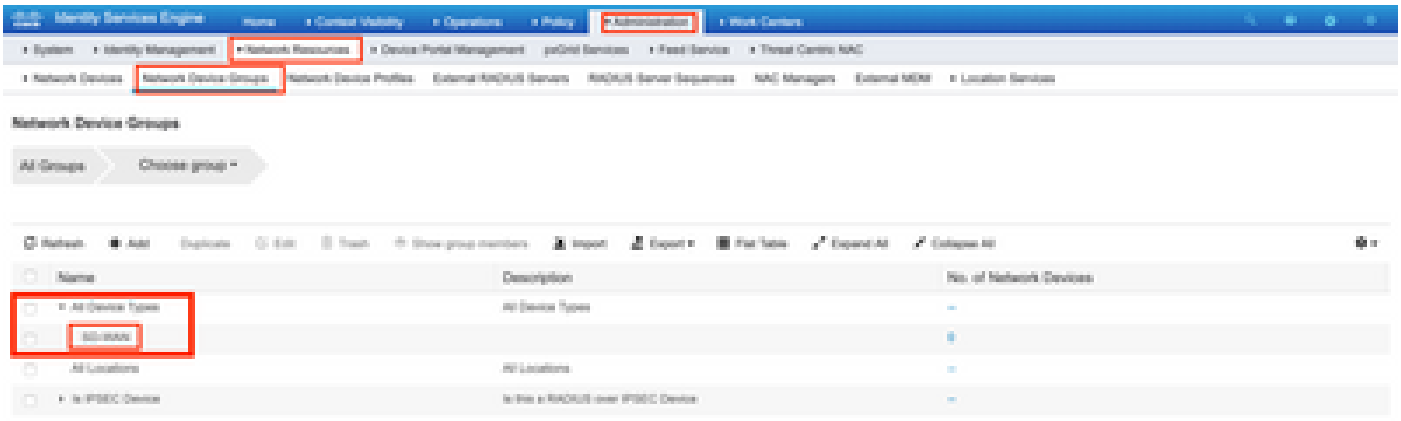
الخطوة 1. إنشاء ملف تعريف TACACS. في هذه الخطوة، يتم تعيين ملف تعريف TACACS الذي تم إنشاؤه، على سبيل المثال، مستوى امتياز NetAdmin لمستخدم تمت مصادقته.

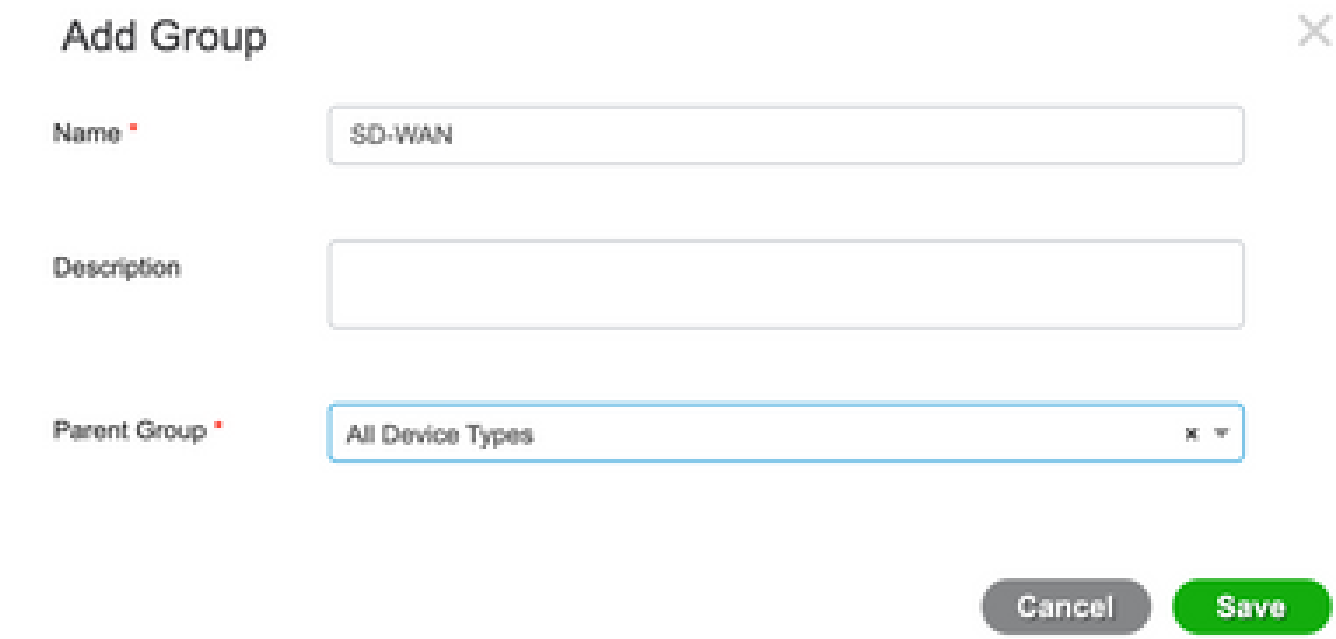
- حدد إلزامي من قسم السمة المخصصة لإضافة السمة ك:

النوع	الاسم	القيمة
إلزامي	اسم مجموعة الفيديو Viptela	Netadmin

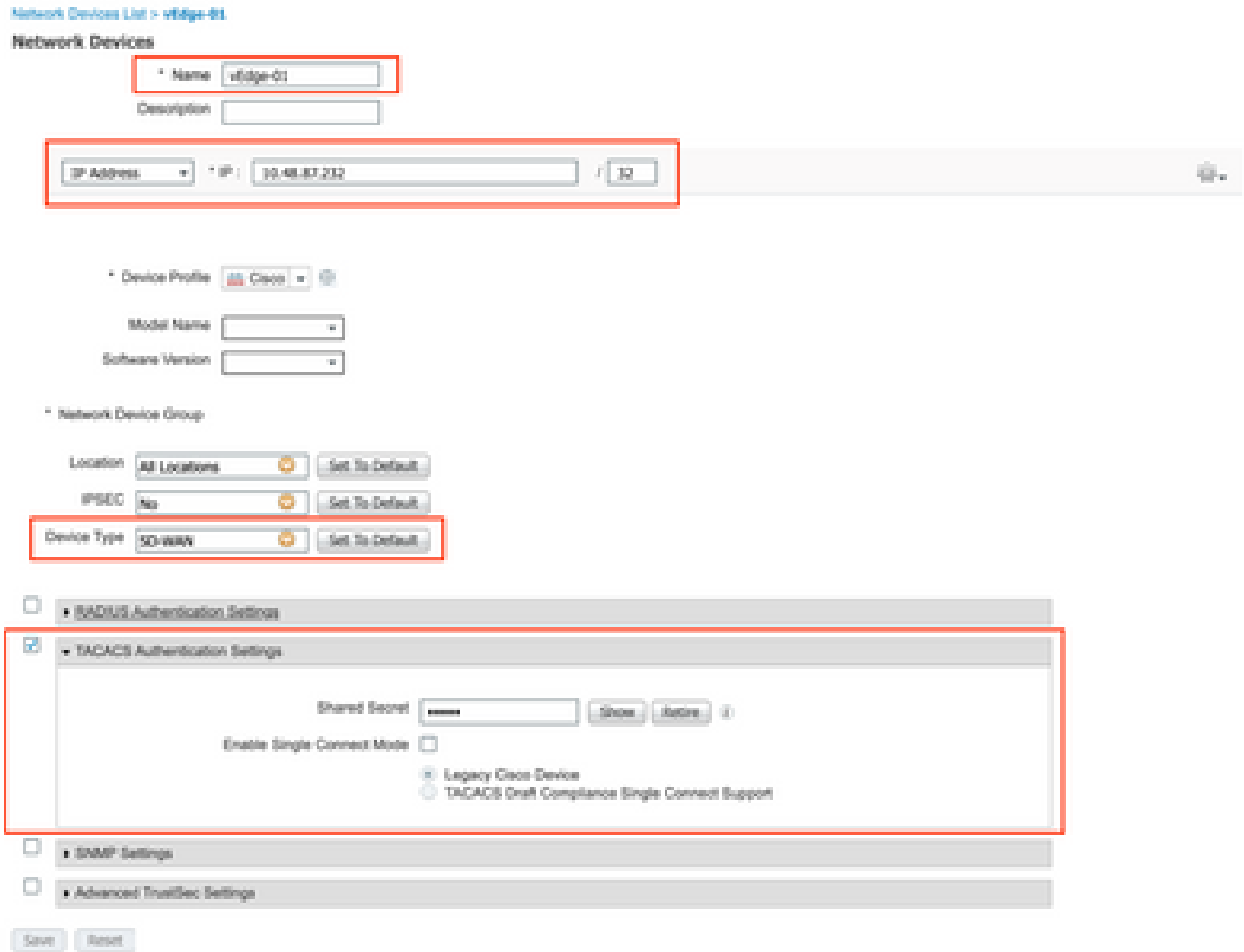


الخطوة 2. إنشاء مجموعة أجهزة ل SD-WAN.



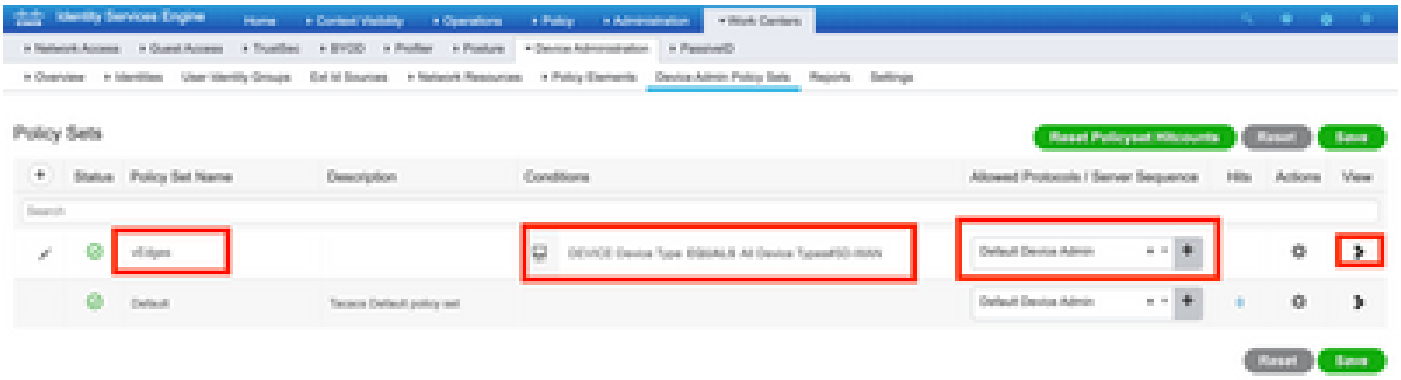


الخطوة 3. قم بتكوين الجهاز وتعيينه إلى مجموعة أجهزة SD-WAN:

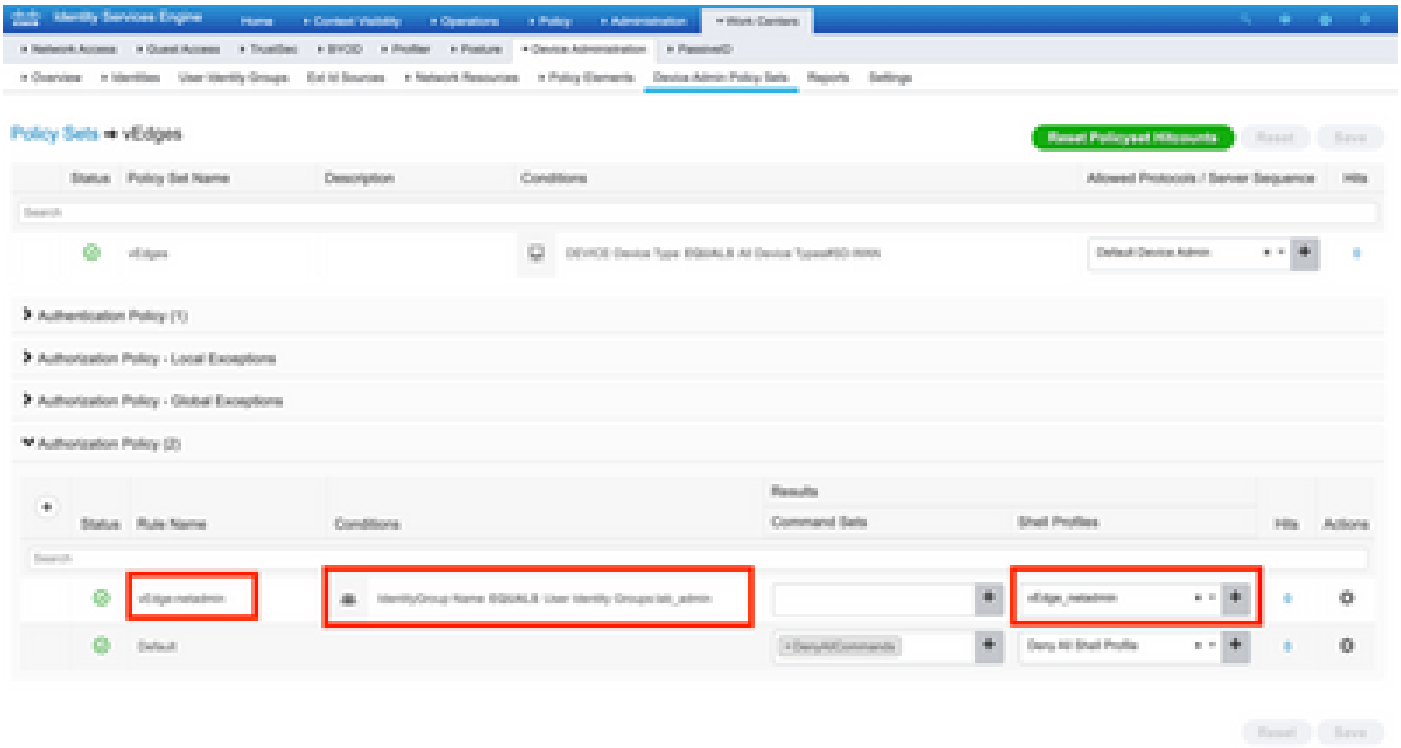


الخطوة 4. تحديد نهج إدارة الأجهزة.

قد تبدو مجموعة النهج بشكل مختلف وفقا للإعداد الفعلي الخاص بك. لأغراض العرض التوضيحي في هذا المستند، يتم إنشاء السياسة.



انقر فوق > وتظهر الشاشة التالية كما هو موضح في هذه الصورة. يتطابق هذا النهج مع نوع الجهاز المسمى SD-WAN ويعين ملف تعريف Shell الذي يتم إنشاؤه في الخطوة 1.



الخطوة 5. تكوين vEdge:

```
system
 aaa
  auth-order tacacs local
 !
 tacacs
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

الخطوة 6. التحقق. قم بتسجيل الدخول إلى برنامج vEdge وتأكد من تعيين مجموعة NetAdmin للمستخدم البعيد:

```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

معلومات ذات صلة

- دليل النشر التعريفي لإدارة أجهزة Cisco ISE: https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973
- تكوين وصول المستخدم والمصادقة: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).